歪多項式環の分離多項式 (代数系アルゴリズムと言語および計算理論)

AUTHOR(S):

池畑, 秀一

CITATION:

池畑, 秀一. 歪多項式環の分離多項式 (代数系アルゴリズムと言語および計算理論). 数理解析研究所講究録 2009, 1655: 11-21

ISSUE DATE:

2009-06

URL:

http://hdl.handle.net/2433/140862

数理解析研究所講究録
第1655巻 2009年 11-21

歪多項式環の分離多項式

岡山大学・大学院自然科学研究科　池畑　秀一 (Shûichi IKEHATA)
Graduate School of Natural Science and Technology
Okyama University

1. 序と準備

本論文は筆者による最近の論文 [12, 13, 14, 16] の概説である.

[17] においてG. J. Janusz は, 体の分離多項式を拡張して可換環の上の分離多項式を最初に考察した. 引き続き [24, 25] 等で, 永原賢は可換環上の分離多項式について研究した. [3] において, 平田和彦と菅野孝三は分離多元環の概念を拡張して環の分離拡大を考察した. この論文では, 歪多項式環のモニックな多項式によって生成されるイデアルの剰余環として現れる環拡大で分離拡大や H-分離拡大となっているものを調べる.

本論を通して, B は単位元1を持つ環とし, Z は B の中心, ρ を B の自己同型写像, D は B の ρ-微分 (ρ-derivaiton) とする. すなわち, D は B から B への加法的写像で $D(\alpha\beta) = \alpha D(\beta) + D(\alpha)\rho(\beta)$ $(\alpha, \beta \in B)$ を満たすものとする. $B[X; \rho, D]$ をその乗法が $\alpha X = X\rho(\alpha) + D(\alpha)$ $(\alpha \in B)$ によって定まる歪多項式環とする. 環の拡大 A/B が分離拡大 (separable extension) であるとは $A \otimes_B A$ から A への A-A-準同型写像 $a \otimes b \to ab$ が分解 (splits) することである. また A/B が H-分離拡大 (H-separable extension) であるとは $A \otimes_B A$ が A の有限個の直和の直和因子に A-A-同型であることである. 良く知られているように H-分離拡大は分離拡大である. H-分離拡大は東屋多元環の概念の一般化として平田和彦によって導入された. 東屋多元環とは中心上分離拡大となっている多元環のことである. 菅野孝三は一貫して H-分離拡大を研究し続けた.

f を歪多項式環 $B[X; \rho, D]$ のモニックな多項式で $fB[X; \rho, D] = B[X; \rho, D]f$ を満たすものとする. このとき剰余環 $B[X; \rho, D]/fB[X; \rho, D]$ は B の free な拡大環となる.

$B[X; \rho, D]/fB[X; \rho, D]$ が B 上分離拡大 (resp.H-分離拡大) のとき,
f を歪多項式環 $B[X; \rho, D]$ における分離多項式 (resp.H-分離多項式) という.

これらは分離拡大や H-分離拡大の典型的な, また本質的な例を与える. 岸本量夫, 永原賢, 宮下庸一, そして筆者は多岐にわたって歪多項式環の分離多項式について研究してきた. 巻末の文献表を参照されたい.

$D = 0$ の場合を自己同型型といい $B[X; \rho, 0] = B[X; \rho]$ と表し,
$\rho = 1_B$ の場合を微分型といい $B[X; 1_B, D] = B[X; D]$ と表す.

一般の場合は極めて計算が困難であるからまずこれら2つの場合に調べるのが常である. 一般の場合は $\rho D = D\rho$ を満たす場合に永原賢 ([27, 28]) によって2次の多項式の場合に試みがあるのみである.

[7] で, 筆者は自己同型型の歪多項式環 $B[X; \rho]$ が素数次数 p の H-分離多項式を含むための必要十分条件は B の中心 Z が Z^ρ 上の $< \rho|Z >$-ガロア拡大であることを証

明した. その後 [33] で, G. Szeto と L. Xue は一般次数でも同じことが成り立つことを示した. しかしながら, 微分型歪多項式環においては状況がパラレルであるようには思えない.

ここでの目的は微分型の分離多項式や H-分離多項式について考察することである. [10] で示されているように, $B[X;D]$ が次数 2 以上の H-分離多項式を含めば, 必然的に B は素数標数となる. したがって**以下 B は素数標数 p であると仮定することにする.**

この論文を通じて, $f = X^p - Xa - b \in B[X;D]$ を中心に考えることにする.

[4, Corollary 1.7] において示されているように, $fB[X;D] = B[X;D]f$ という条件は次と同値である.

$$D(a) = D(b) = 0, \quad a \in Z \quad \text{and} \quad D^p(\alpha) - D(\alpha)a = \alpha b - b\alpha \quad (\alpha \in B).$$

以後次の記号を用いることにする:

$B[X;D]_{(0)} = B[X;D]$ のモニック多項式 g で $gB[X;D] = B[X;D]g$ を満たすものの全体の集合.

$B^D = \{\alpha \in B \mid D(\alpha) = 0\}, Z^D = \{\alpha \in Z \mid D(\alpha) = 0\}$.

$D^* : B[X;D] \to B[X;D]$ は $B[X;D]$ の X によって定まる内部微分, すなわち $D^*(\Sigma_i X^i d_i) = \Sigma_i X^i D(d_i)$.

後の部分で用いる結果をまとめておく.

微分型歪多項式環における分離多項式については, すでに宮下庸一によって次の特徴付けが得られている.

補題 1.1. ([23, Theorem 3.2]) $f = X^p - Xa - b \in B[X;D]_{(0)}$ とする. このとき f が $B[X;D]$ における分離多項式であるための必要十分条件は, ある適当な $y = X^{p-1}d_{p-1} + X^{p-2}d_{p-2} + \cdots + Xd_1 + d_0 \in B[X;D]$ が存在して $\alpha y = y\alpha$ $(\alpha \in B)$ および $D^{*p-1}(y) - ya = 1$ が成り立つことである.

[4] において, 筆者は上の結果を p-多項式の場合に拡張した.

補題 1.2. ([4, Theorem 4.1]) $f = X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1 + \alpha_0 \in B[X;D]_{(0)}$ とする. このとき f が $B[X;D]$ における分離多項式であるための必要十分条件は, ある適当な $y = X^{p^e-1}d_{p^e-1} + X^{p^e-2}d_{p^e-2} + \cdots + Xd_1 + d_0 \in B[X;D]$ が存在して $\alpha y = y\alpha$ $(\alpha \in B)$ および $D^{*p^e-1}(y) + D^{*p^{e-1}-1}(y)\alpha_e + \cdots + D^{*p-1}(y)\alpha_2 + D*(y)\alpha_1 = 1$ が成り立つことである.

[5] において, 筆者は H-分離多項式に関して次の特徴付けを得た.

補題 1.3. ([5, Lemma 1.5]) $f = X^p - Xa - b \in B[X;D]_{(0)}$ とし, $I = fB[X;D]$ とする. このとき f が $B[X;D]$ における H-分離多項式であるための必要十分条件は, ある適当な $y_i, z_i \in B[X;D]$ で $\deg y_i < p$, $\deg z_i < p$, $\alpha y_i = y_i\alpha$, $\alpha z_i = z_i\alpha$ $(\alpha \in B)$ および

$$\sum_i D^{*p-1}(y_i)z_i \equiv 1 \pmod{I}, \quad \sum_i D^{*k}(y_i)z_i \equiv 0 \pmod{I} \ (0 \le k \le p-2)$$

を満たすものが存在することである.

2. 分離多項式

[24] で永原賢は, $D=0$ のとき, すなわち通常の多項式環で $f=X^p-Xa-b\in B[X]_{(0)}$ が分離多項式であるための必要十分条件は $f'=-a$ が Z で可逆であることであることを示した. よって補題 1.1 はこの結果の一般化となっている. このときは, 補題 1.1 で y は Z の中でとれている. この節では補題 1.1 における y がどのような場合に Z の中でとれるかについて調べる.

次の条件を考える:
(C_1) B は可換環である.
(C_2) $D(Z)$ で生成される Z のイデアルは非零因子を含む.
(C_3) Z は半素環 (semiprime ring) である.

補題 1.1 から直ちに次を得る.

命題 2.1. $f=X^p-Xa-b\in B[X;D]_{(0)}$ とする. (C_1) または (C_2) が成立つとき, f が $B[X;D]$ における分離多項式であるための必要十分条件は, 適当な元 $z\in Z$ が存在して $D^{p-1}(z)-za=1$ が成り立つことである.

証明. $f=X^p-Xa-b$ を分離多項式とする. $y=X^{p-1}d_{p-1}+X^{p-2}d_{p-2}+\cdots+Xd_1+d_0$ を補題 1.1 におけるものとする. (C_1) の場合は, y の定数項を z とすればよい. 次に (C_2) を仮定する. $\alpha y=y\alpha$ ($\alpha\in B$) により,

$$\alpha d_{p-1}=d_{p-1}\alpha \quad \text{かつ} \quad (p-1)D(\alpha)d_{p-1}=d_{p-2}\alpha-\alpha d_{p-2}$$

を得る. 仮定から $u_i,v_i\in Z$ で $\sum_i D(u_i)v_i=c$ が Z の非零因子となるものが存在する. $D(u_i)d_{p-1}=0$ であるから, $\sum_i D(u_i)v_id_{p-1}=cd_{p-1}=0$ となる. よって $d_{p-1}=0$. これを繰り返せば $y=d_0\in Z$ がわかる. 逆は補題 1.1 から自明である.

次の定理は筆者が [13] で提出した問題の肯定的な解決である. そこでは $p=3$ の場合に証明し、任意の素数 p で成り立つかどうか問題を提起していた.

定理 2.2. ([14, Theorem 2.2]) $f=X^p-Xa-b\in B[X;D]_{(0)}$ とし, Z を半素環とする. そのとき f が $B[X;D]$ における分離多項式であるための必要十分条件は, ある適当な元 $z\in Z$ が存在して $D^{p-1}(z)-az=1$ となることである.

証明. f を $B[X;D]$ の分離多項式とする. 補題 1.1 により, 適当な $y=X^{p-1}d_{p-1}+X^{p-2}d_{p-2}+\cdots+Xd_1+d_0\in B[X;D]$ が存在して $\alpha y=y\alpha$ ($\alpha\in B$) および $D^{*p-1}(y)-ya=1$ を満たす. このとき次が成り立つ.

(1) $$d_{p-1}\in Z,\ (p-1)D(\alpha)d_{p-1}+\alpha d_{p-2}=d_{p-2}\alpha\ (\alpha\in B).$$

(2) $$D^{p-1}(\alpha)d_{p-1}+D^{p-2}(\alpha)d_{p-2}+\cdots+D(\alpha)d_1+\alpha d_0=d_0\alpha\ (\alpha\in B).$$

(3) $$D^{p-1}(d_k)-d_ka=0\ (1\le k\le p-1).$$

(4) $$D^{p-1}(d_0)-d_0a=1.$$

最初に $d_{p-1}=0$ となることを示そう.
(1) により,

$$(p-1)D(\alpha)D(d_{p-1})+\alpha D(d_{p-2})=D(d_{p-2})\alpha\ (\alpha\in B)$$

となる. 上の式に $\alpha = d_{p-1} \in Z$ を代入することにより, $\{D(d_{p-1})\}^2 = 0$ を得る. Z は半素環であるから, $D(d_{p-1}) = 0$ となる. (1) に $\alpha = d_{p-2}$ を代入して, $D(d_{p-2})d_{p-1} = 0$ がわかる. このことにより

$$D^k(d_{p-2})d_{p-1} = 0 \ (k = 1, 2, 3, \cdots) \tag{5}$$

となることがわかる.

(1) と (2) から,

$$\begin{aligned} D(d_0)d_{p-1} &= d_0 d_{p-2} - d_{p-2}d_0 \\ &= D^{p-1}(d_{p-2})d_{p-1} + D^{p-2}(d_{p-2})d_{p-2} + \cdots + D(d_{p-2})d_1. \end{aligned}$$

したがって (5) より,

$$\begin{aligned} D(d_0)d_{p-1}^2 &= \{D^{p-1}(d_{p-2})d_{p-1} + D^{p-2}(d_{p-2})d_{p-2} + \cdots + D(d_{p-2})d_1\}d_{p-1} \\ &= D^{p-1}(d_{p-2})d_{p-1}^2 + D^{p-2}(d_{p-2})d_{p-1}d_{p-2} + \cdots + D(d_{p-2})d_{p-1}d_1 \\ &= 0. \end{aligned}$$

$D(d_{p-1}) = 0$ であるから,

$$D^k(d_0)d_{p-1}^2 = 0 \ (k = 1, 2, 3, \cdots) \tag{6}$$

となる.

(3) と (4) を用いると,

$$\begin{aligned} d_{p-1} &= \{D^{p-1}(d_0) - d_0 a\}d_{p-1} \\ &= D^{p-1}(d_0)d_{p-1} - d_0(ad_{p-1}) \\ &= D^{p-1}(d_0)d_{p-1} - d_0 D^{p-1}(d_{p-1}) \\ &= D^{p-1}(d_0)d_{p-1}. \end{aligned}$$

したがって (6) により $d_{p-1}^2 = D^{p-1}(d_0)d_{p-1}^2 = 0$. Z は半素環であるから, $d_{p-1} = 0$ となる. この方法を繰り返せば $d_{p-2} = \cdots = d_1 = 0$ であることがわかる. よって $y = d_0 \in Z$ となる. これで証明が終わる.

3. H-分離多項式

この節では H-分離多項式について考える. 補題 1.3 における $\{y_i, z_i\}$ がいつ Z の中でとれるのか調べよう.

最初に, 次の定理を証明しよう.

定理 3.1. ([14, Theorem 3.1]) $f = X^p - Xa - b \in B[X; D]_{(0)}$ とする. Z を半素環とする. このとき f が $B[X; D]$ における H-分離多項式であるためには, ある適当な元 $y_i, z_i \in Z$ が存在して

$$\sum_i D^{p-1}(y_i)z_i = 1, \quad \sum_i D^k(y_i)z_i = 0 \ \ (0 \leq k \leq p-2)$$

が成り立つことである.

証明. 補題 1.3 により, 次のことを示せば十分である:
$y = X^{p-1}d_{p-1} + X^{p-2}d_{p-2} + \cdots + Xd_1 + d_0$ を $B[X;D]$ の元で $\alpha y = y\alpha$ $(\alpha \in B)$ を満たすものとするとき, $y = d_0$ となる, すなわち, $y \in Z$ である.
$\alpha y = y\alpha$ $(\alpha \in B)$ と仮定する. このとき

$$\alpha d_{p-1} = d_{p-1}\alpha, \quad (p-1)D(\alpha)d_{p-1} + \alpha d_{p-2} = d_{p-2}\alpha$$

かつ

$$D(d_{p-2})d_{p-1} = 0, \quad D(d_{p-1})d_{p-1} = 0$$

を得る. それゆえ

$$(p-1)D(\alpha)d_{p-1}^3 = d_{p-2}d_{p-1}^2\alpha - \alpha d_{p-2}d_{p-1}^2 \ (\alpha \in B),$$

かつ

$$\begin{aligned} D(d_{p-2}d_{p-1}^2) &= D(d_{p-2})d_{p-1}^2 + d_{p-2}D(d_{p-1}^2) \\ &= D(d_{p-2})d_{p-1}^2 + 2d_{p-2}D(d_{p-1})d_{p-1} \\ &= 0 \end{aligned}$$

が成り立つ. したがって [10, Lemma 2.1] により, $(p-1)d_{p-1}^3 = 0$ となる, よって $d_{p-1}^3 = 0$. Z は半素環であるから, $d_{p-1} = 0$ となる. この手続きを繰り返して, $d_{p-2} = d_{p-3} = \cdots = d_1 = 0$ となることがわかる. このようにして $y = d_0 \in Z$. これで証明をおわる.

次の条件を思い出そう:
(C_1) B は可換環である.
(C_2) $D(Z)$ で生成される Z のイデアルは非零因子を含む.
(C_3) Z は半素環 (semiprime ring) である.

次は岡本浩明と筆者による [32, Theorem 8] の一般化である.

定理 3.2. ([14, Theorem 3.2]) $(C_1)-(C_3)$ のうちのどれかひとつの条件が成り立つものとする. このとき次は同値である:
(1) $B[X;D]$ は次数 p の H-分離多項式 f を含む.
(2) $B[X;D]_{(0)}$ は次数が p の多項式を含み, Z は rank p の射影的 Z^D-加群となり, $\mathrm{Hom}({}_{Z^D}Z, {}_{Z^D}Z) = Z[D|Z]$, すなわち, Z/Z^D は S. Yuan([34]) の意味での指数 1 の純非分離拡大である.
(3) $B[X;D]_{(0)}$ は次数 p の多項式を含み, また適当な元 $y_i, z_i \in Z$ が存在して

$$\sum_i D^{p-1}(y_i)z_i = 1, \quad \sum_i D^k(y_i)z_i = 0 \ \ (0 \le k \le p-2)$$

が成り立つ.
このとき, $\{g \mid g$ は $B[X;D]$ における H-分離多項式 $\} = \{f + c \mid c \in Z^D\} = \{g \mid g$ は $B[X;D]_{(0)}$ における次数 p の多項式 $\}$.

証明. [5, Theorem 3.3] の証明を注意深く検討すれば (2) と (3) の同値性は $(C_1)-(C_3)$ のどの条件がなくても成り立つことが分かる.
(3) $\Rightarrow$ (1) は補題 1.3 から分かる.

残っているのは (1) ⇒ (3) を示すことだけである. [5, Theorem 3.3] から, (C_1) の場合は自明である. (C_2) のとき, 命題 2.1 の証明の中で, $y = X^{p-1}d_{p-1} + X^{p-2}d_{p-2} + \cdots + Xd_1 + d_0 \in B[X;D]$ が $\alpha y = y\alpha$ $(\alpha \in B)$ を満たせば,$y = d_0$, すなわち, $y \in Z$ となることを示した. よって補題 1.3 における $\{y_i, z_i\}$ は Z の中でとれる.

(C_3) の場合は定理 3.1 ですでに示した. 残りの部分は [10, Proposition 2.3] からわかる.

4. H-分離多項式とガロア多項式

この節の目的は $B[X;D]$ における多項式 $f = X^p - Xa - b$ がいつ H-分離多項式となるのかの, 分かりやすい十分条件を与えることである. 補題 1.3 は $f = X^p - Xa - b$ が H-分離多項式であるための必要十分条件を与えているものの, 決してチェックしやすい条件ではない. ある簡明な条件を満たせば f が H-分離多項式であるという形の定理を与える. ここでは次の定理を示そう: $f = X^p - Xa - b \in B[X;D]_{(0)}$ とする. もし B の中心 Z が元 z で $D(z)$ が可逆となるものを含めば,f は $B[X;D]$ における H-分離多項式である. さらに, z も可逆元であるときには, f は $B[X;D]$ におけるガロア多項式となる.

ここでガロア多項式の定義をしておかなければならない. 環の拡大 A/B が G-ガロア拡大であるとは, A の自己同型から成る有限群 G に対して $B = A^G$(A における G の固定環) となり, 適当な元 $x_i, y_i \in A$ が存在して $\sum_i x_i\sigma(y_i) = \delta_{1,\sigma}$ $(\sigma \in G)$ が成立つとき言う. ここで $\delta_{1,\sigma}$ はクロネッカーのデルタである. $\{x_i, y_i\}$ のことを A/B の G-ガロアシステムと言う. 良く知られているように G-ガロア拡大は分離拡大である. f を $B[X;D]$ のモニック多項式で $fB[X;D] = B[X;D]f$ を満たすものとする. このとき f が $B[X;D]$ におけるガロア多項式であるとは, 適当な有限群 G に対して,$B[X;D]/fB[X;D]$ が B 上で G-ガロア拡大となっているとき言う. ある H-分離多項式はガロア多項式となることを示そう.

ガロア多項式に関しては, 次の岸本量夫による補題が基本的である.

補題 4.1. ([18, Theorem 1.1 and Corollary 1.1]) $f = X^p - X - b \in B[X;D]_{(0)}$ とする. このとき f は $B[X;D]$ におけるガロア多項式である.

証明. 証明のアウトラインを示しておく.

$S = B[X;D]/fB[X;D]$ とする, ここで $x = X + fB[X;D] \in S$ である.

写像 $\sigma : S \to S$ を $\sigma(\sum_i x^i d_i) = \sum_i (x+1)^i d_i$ によって定義すれば,σ は S の位数 p の B-自己同型である. $G = <\sigma>$ とおく. このとき $S^G = B$ となることは容易に示せる.

$$a_j = j^{-1}\sigma^j(x) \quad \text{かつ} \quad b_j = (-j^{-1})x \quad (1 \le j \le p-1)$$

と置く. このとき

$$\Pi_{j=1}^{p-1}(a_j + b_j) = 1 \quad \text{かつ} \quad \Pi_{j=1}^{p-1}(a_j + \sigma^k(b_j)) = 0 \quad (1 \le k \le p-1)$$

の展開式から S/B の G-ガロアシステムを得ることができる. このようにして, S は B の G-ガロ拡大である. これで証明を終わる.

主定理 (定理 4.4) を示すために, まず特別な場合を示す.

補題 4.2. $f = X^p - Xa - b \in B[X;D]_{(0)}$ とする. 適当な元 $z \in Z$ が存在して $D(z) = 1$ となれば,$f = X^p - b$, すなわち, $a = 0$, となり f は $B[X;D]$ における H-分離多項式である. さらに,z も Z の可逆元であれば, f は $B[X;D]$ におけるガロア多項式である.

証明. 補題 1.1 の直前で注意したように,

$$D^p(\alpha) - D(\alpha)a = \alpha b - b\alpha \quad (\alpha \in B)$$

となる. 上式において $\alpha = z$ を代入する. このとき $D(z) = 1$ であるから,$a = 0$ を得る. $0 \leq i \leq p-1$ に対して,$x_i = -z^i, y_i = z^{p-i-1}$ と置く. このとき, 容易に次のことを示すことができる.

$$\sum_{i=0}^{p-1} D^{p-1}(x_i)y_i = 1 \quad \text{かつ} \quad \sum_{i=0}^{p-1} D^k(x_i)y_i = 0 \quad (0 \leq k \leq p-2).$$

それゆえ補題 1.3 により,$f = X^p - b$ は $B[X;D]$ における H-分離多項式である.

次に,z が Z の可逆元であるとする.B の微分 $\Delta = z_\ell D = zD$ を考える. このとき $D(z) = 1$ であるから,$\Delta(z) = z$ となる. よって有名な Hochschild の公式により,

$$\begin{aligned}\Delta^p = (zD)^p &= z^p D^p + (zD)^{p-1}(z)D \\ &= z^p D^p + zD = z^p I_b + \Delta \\ &= \Delta + I_{z^p b}\end{aligned}$$

を得る. ここで $Y = zX$ と置けば,

$$\alpha Y = Y\alpha + \Delta(\alpha) \quad (\alpha \in B)$$

を得る. それゆえ $B[X;D] = B[Y;\Delta]$ かつ $Y^p = (zX)^p = (Xz+1)^p = (Xz)^p + 1 = X^p z^p + Xz + 1$ がわかる. よって $Y^p - Y = (X^p z^p + Xz + 1) - (Xz+1) = X^p z^p = (f+b)z^p = fz^p + bz^p$ となる. 補題 4.1 から $g = Y^p - Y - bz^p = fz^p$ は $B[Y;\Delta]$ におけるガロア多項式である. $B[X;D] = B[Y;\Delta]$ かつ $fB[X;D] = B[X;D]f = gB[Y;\Delta] = B[Y;\Delta]g$ であることに注意すれば, f もまた $B[X;D]$ におけるガロア多項式であることがわかる.

次は補題 4.2 から直ちにわかる.

系 4.3. $f = X^p - b \in B[X;D]_{(0)}$ とする. 適当な元 $z \in Z$ が存在して $D(z) = 1$ となれば, f は $B[X;D]$ における H-分離多項式である. さらに,z も Z の可逆元であれば, f は $B[X;D]$ におけるガロア多項式である.

次がこの節の主定理であるる.

定理 4.4. ([12, Theorem 3.3]) $f = X^p - Xa - b \in B[X;D]_{(0)}$ とする. 適当な元 $z \in Z$ が存在して $D(z)$ が Z の可逆元であれば,f は $B[X;D]$ における H-分離多項式である. さらに,z も Z の可逆元であれば, f は $B[X;D]$ におけるガロア多項式である.

証明. 適当な $c \in Z$ に対して $cD(z) = 1$ と仮定する.$\Delta = cD$ と置く. このとき $\Delta(z) = 1$ であるから,

$$\begin{aligned}\Delta^p &= (cD)^p = c^p D^p + (cD)^{p-1}(c)D \\ &= c^p(aD + I_b) + \Delta^{p-1}(c)D \\ &= (c^{p-1}a + \Delta^{p-1}(c)c^{-1})\Delta + I_{c^p b}.\end{aligned}$$

$\Delta(z) = 1$ であるから,$c^{p-1}a + \Delta^{p-1}(c)c^{-1} = 0$ となる. よって $\Delta^p = I_{bc^p}$, $bc^p \in B^\Delta$ となる. ここで $Y = cX$ と置く. このとき

$$\alpha Y = Y\alpha + \Delta(\alpha) \quad \text{かつ} \quad \alpha Y^p = Y^p\alpha + \Delta^p(\alpha) \quad (\alpha \in B)$$

となる. それゆえ $B[X;D] = B[Y;\Delta]$ となり $Y^p - bc^p = c^p f$ となる. よって前の系 4.3 より, $Y^p - bc^p$ は $B[Y;\Delta]$ における H-分離多項式かつガロア多項式となる. したがって f はまた $B[X;D]$ における H-分離多項式かつガロア多項式である.

次の系は定理 4.4 から直ちに得られる.

系 4.5. B を単純環とし $D|Z \neq 0$ とすれば, 任意の $f = X^p - Xa - b \in B[X;D]_{(0)}$ はいつでも $B[X;D]$ における H-分離多項式かつガロア多項式である.

系 4.6. B を体とし $D \neq 0$ とすれば, 任意の $f = X^p - Xa - b \in B[X;D]_{(0)}$ はいつでも $B[X;D]$ における H-分離多項式かつガロア多項式である.

ここでひとつ例をあげておこう.

例 4.7. k を素数標数 p の体とし,$B = k[t]$ を一変数多項式環とする. $D = \frac{d}{dt}$ とすると, $D^p = 0$, $D(t) = 1$ そして $B^D = k[t^p]$ となる. このとき任意の $u \in k[t^p]$ に対して, $f = X^p - u$ は $B[X;D]$ における H-分離多項式である. $B' = k[t,t^{-1}]$ とし, D の B' への自然な拡張を同じ D で表せば, 任意の $u \in k[t^p,t^{-p}]$ に対して, $f = X^p - u$ は $B'[X;D]$ における H-分離多項式かつガロア多項式である. 次に,$\Delta = t\frac{d}{dt}$ とすると,$\Delta^p - \Delta = 0, \Delta(t) = t$ そして $B^\Delta = k[t^p]$ となる. このとき任意の $u \in k[t^p]$ に対して, $g = Y^p - Y - u$ は $B[Y;\Delta]$ におけるガロア多項式である. しかしながら,$\Delta^{p-1}(B)$ によって生成される B のイデアルは B に一致しないから,[5, Theorem 3.1] から g は $B[Y;\Delta]$ における H-分離多項式とはならない.

5. $D|Z = 0$ の場合

[6] で, 筆者は次の結果を示した: $D|Z = 0$ とする. $f = X^p - Xa - b \in B[X;D]_{(0)}$ とする. このとき f が $B[X;D]$ における分離多項式であるための必要十分条件は,a が B の可逆元であることである.

この事実は次のように一般化できる.

定理 5.1. ([16, Theorem 2.1]) $D|Z = 0$ とする. $f = X^{p^e} - Xa - b \in B[X;D]_{(0)}$, ここで e は任意の正の整数とする. このとき f が $B[X;D]$ における分離多項式であるための必要十分条件は,a が B の可逆元であることである.

証明. [4, Corollary 1.7] で示されているように,$fB[X;D] = B[X;D]f$ という条件は次と同値である:

$$D(a) = D(b) = 0, \quad a \in Z \quad \text{and} \quad D^{p^e}(\alpha) - D(\alpha)a = \alpha b - b\alpha \quad (\alpha \in B).$$

f を $B[X;D]$ における分離多項式とすると, 補題1.2により適当な元 $y = X^{p^e-1}d_{p^e-1} + X^{p^e-2}d_{p^e-2} + \cdots + Xd_1 + d_0 \in B[X;D]$ が存在して $\alpha y = y\alpha$ $(\alpha \in B)$ および $D^{*p^e-1}(y) - ya = 1$ を満たす. 明らかに, $\alpha y = y\alpha$ $(\alpha \in B)$ から $d_{p^e-1} \in Z$ がわかる, したがって $D(d_{p^e-1}) = 0$.

数学的帰納法により

$$\alpha D^{*k-1}(y) = D^{*k-1}(y)\alpha \quad (\alpha \in B) \tag{7}$$

かつ

$$D^k(d_{p^e-k}) = 0 \quad (1 \le k \le p^e) \tag{8}$$

となることがわかる.

(7) と (8) より

$$D(\alpha)D^{p^e-2}(d_1) + \alpha D^{p^e-2}(d_0) = D^{p^e-2}(d_0)\alpha \ (\alpha \in B), \quad D^{p^e-2}(d_1) \in Z. \tag{9}$$

さらに, $D^{*p^e-1}(y) - ya = 1$ から

$$D^{p^e-1}(d_0) - d_0 a = 1. \tag{10}$$

$$-d_1 a = 0. \tag{11}$$

(9) に $\alpha = D^{p^e-2}(d_0)$ を代入することにより,

$$D^{p^e-1}(d_0)D^{p^e-2}(d_1) = 0 \tag{12}$$

がわかる.

(9), (10), (11), および (12) から,

$$\begin{aligned} D^{p^e-2}(d_0)\alpha - \alpha D^{p^e-2}(d_0) &= D(\alpha)D^{p^e-2}(d_1) \\ &= D(\alpha)\{D^{p^e-1}(d_0) - d_0 a\}D^{p^e-2}(d_1) \\ &= D(\alpha)\{D^{p^e-1}(d_0)D^{p^e-2}(d_1) - d_0 D^{p^e-2}(ad_1)\} \\ &= 0. \end{aligned}$$

となる.

したがって, $D^{p^e-2}(d_0) \in Z$ となり, (10) から, $1 = D^{p^e-1}(d_0) - ad_0 = -ad_0$, よって a は B の可逆元である.

逆に,a が B の可逆元であるとする. 前に注意したように $a \in Z^D$ であるから,$D(a^{-1}) = 0$ である. $y = -a^{-1}$ とおけば, $D^{p^e-1}(y) - ya = 1$ かつ $\alpha y = y\alpha$ $(\alpha \in B)$ を得る. したがって, 補題1.2から f は $B[X;D]$ における分離多項式である.

定理5.1から直ちに,[14, Theorem 3.3] の一般化である次の結果を得る.

定理 5.2. $D|Z = 0$ とする. $f = X^{p^e} - Xa - b \in B[X;D]_{(0)}$ とする. このとき f は決して $B[X;D]$ における H-分離多項式ではない. 換言すれば, $X^{p^e} - Xa - b$ の形をした $B[X;D]$ における H-分離多項式は存在しない.

証明. f を $B[X;D]$ における H-分離多項式とする. 最初に次のことを示そう:
$y = X^{p^e-1}d_{p^e-1} + X^{p^e-2}d_{p^e-2} + \cdots + Xd_1 + d_0 \in B[X;D]$ が $\alpha y = y\alpha$ $(\alpha \in B)$ を満たすならば, $D^*(y) = 0$ である.

$D|Z = 0$ であるから, 定理5.1の証明の中で示したように, $D^k(d_{p^e-k}) = 0$ $(1 \leq k \leq p^e)$ が成り立つ. したがって $D^{*p^e}(y) = 0$ がわかる. $D^{*p^e}(y) - D^*(y)a = yb - by = 0$ であるから, $D^*(y)a = 0$ を得る. f は H-分離多項式であるから, 分離多項式でもある. したがって定理5.1により, a は B の可逆元であるから, $D^*(y) = 0$ となる.

[5, Lemma 1.5] から, ある適当な元 $y_i, z_i \in B[X;D]$ が存在して $\deg y_i < m$, $\deg z_i < m$, $\alpha y_i = y_i\alpha$, $\alpha z_i = z_i\alpha$ $(\alpha \in B)$ かつ

$$\sum_i D^{*m-1}(y_i)z_i \equiv 1 \pmod{I}, \quad \sum_i D^{*k}(y_i)z_i \equiv 0 \pmod{I} \ (0 \leq k \leq m-2)$$

が成り立つ. しかしながら, 証明の最初に示したことにより, $D^*(y_i) = 0$ がわかる. したがって $\sum_i D^{*m-1}(y_i)z_i \equiv 1 \pmod{I}$ となることは不可能である. これは矛盾である. よって f は決して H-分離多項式となることはない.

最後に, 次の問題を提起しておく.

問題 1. $D|Z = 0$ とする. $f = X^{p^e} + X^{p^e-1}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1 + \alpha_0$ を $B[X;D]$ における任意の p-多項式で, $fB[X;D] = B[X;D]f$ を満たすものとする. このとき f が $B[X;D]$ における分離多項式であるための必要十分条件は, a が B の可逆元であることであるか?

問題 2. $D|Z = 0$ とする. このとき $B[X;D]$ には (次数2以上の) H-分離多項式は存在しないか?

注意. [10, Theorem 2.2] で示したように, $B[X;D]$ が次数 $m \geq 2$ の H-分離多項式 f を含めば, B は必然的に素数標数 p となり, f は p-多項式となる. すなわち $f = X^{p^e} + X^{p^e-1}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1 + \alpha_0$ で, $m = p^e$ となる. よって問題2では p-多項式のみを考えれば良い.

REFERENCES

[1] S. U. Chase, D. K. Harrison and A. Rosenberg, Galois theory and Galois cohomology ofcommutative ring, *Mem. Amer. Math. Soc.*, **52** 1965, 15–33.

[2] K. Hirata, Separable extensions and centralizers of rings, *Nagoya Math. J.*, **35** 1969, 31–45.

[3] K. Hirata and K. Sugano, On semisimple extensions and separable extensions overnon commutative rings, *J. Math. Soc. Japan,* **18** 1966, no. 2, 360–373.

[4] S. Ikehata, On separable polynomials and Frobenius polynomials in skew polynomial rings, *Math. J. Okayama Univ.*, **22** 1980, 115–129.

[5] S. Ikehata, Azumaya algebras and skew polynomial rings, *Math, J. Okayama Univ.*, **23** 1981, 19–32.

[6] S. Ikehata, A note on separable polynomials in skew polynomial rings ofderivation type, *Math. J. Okayama Univ.*, **22** 1980, 59–60.

[7] S. Ikehata, On H-separable polynomials of prime degree, *Math. J. Okayama Univ.*, **33** 1991, 21–26.

[8] S. Ikehata and G. Szeto, On H-separable polynomials in skew polynomial rings of automorphism type, *Math. J. Okayama Univ.*, **34** 1992, 49–55.

[9] S. Ikehata and G. Szeto, On H-skew polynomial rings and Galois extensions, *Lecture Notes in Pure and Appl. Math.,* **159** Mercel Dekker, Inc., 1994, 113–121.
[10] S. Ikehata, Purely inseparable ring extensions and H-separable polynomials, *Math. J. Okayama Univ.,* **40** 1998, 55–63.
[11] S. Ikehata, Purely inseparable ring extensions and Azumaya algebras, *Math. J. Okayama Univ.,* **41** 1999, 63–69.
[12] S. Ikehata, On H-separable and Galois polynomials of degree p in skew polynomial rings, *Int. Math. Forum,* **3** 2008, no. 29-32, 1581-1586.
[13] S. Ikehata, A note on separable polynomials of degree 3 in skew polynomial rings, *Int. J. Pure Appl. Math.,* **50** 2009, no. 1, 145–149.
[14] S. Ikehata, On separable and H-separable polynomials of degree p in skew polynomial rings, *Int. J. Pure Appl. Math.,* **51** 2009, no.1, 149–156.
[15] S. Ikehata, On separable and H-separable polynomials in skew polynomial rings of several variables, Submitted.
[16] S. Ikehata, A note on separable polynomials of derivation type, Submitted.
[17] G. J. Janusz, Separable algebras over commutative rings, *Trans. Amer. Math. Soc.,* **122** 1966, 461–479.
[18] K. Kishimoto, On abelian extensions of rings. I, *Math. J. Okayama Univ.,* **14** 1970, 159–174.
[19] K. Kishimoto, On abelian extensions of rings. II, *Math. J. Okayama Univ.,* **15** 1971, 57–70.
[20] K. Kishimoto, A classification of free quadratic extensions of rings, *Math. J. Okayama Univ.,* **18** 1976, 139–148.
[21] K. Kishimoto, A classification of free extensions of rings of automorphisim type and derivation type, *Math. J. Okayama Univ.,* **18** 1977, 163–169.
[22] K. Kishimoto, On connectedness of strongly abelian extensions of rings, *Math. J. Okayama Univ.,* **26** 1984, 59–70.
[23] Y. Miyashita, On a skew polynomial ring, *J. Math. Soc. Japan,* **31** 1979, no. 2, 317–330.
[24] T. Nagahara, Characterization of separable polynomials over a commutative ring, *Proc. Japan Acad.,* **46** 1970, 1011–1015.
[25] T. Nagahara, On separable polynomials over a commutative ring, *Math. J. Okayama Univ.,* **14** 1970, 175–181.
[26] T. Nagahara, On separable polynomials of degree 2 in skew polynomial rings, *Math. J. Okayama Univ.,* **19** 1976, 65–95.
[27] T. Nagahara, On separable polynomials of degree 2 in skew polynomial rings , *Math. J. Okayama Univ.,* **21** 1979, 167–177.
[28] T. Nagahara, On separable polynomials of degree 2 in skew polynomial rings , *Math. J. Okayama Univ.,* **22** 1980, 61–64.
[29] T. Nagahara, A note on separable polynomials in skew polynomial rings of atutomorphism type, *Math. J. Okayama Univ.,* **22** 1980, 73–76.
[30] T. Nagahara, Some H-separable polynomials of degree 2, *Math. J. Okayama Univ.,* **26** 1984, 87–90.
[31] T. Nagahara, A note on imbeddings of non-commutative separable extensions in Galois extensions, *Houston J. Math.,* **12** 1986, 411–417.
[32] H. Okamoto and S. Ikehata, On H-separable polynomials of degree 2, *Math. J. Okayama Univ.,* **32** 1990, 53–59.
[33] G. Szeto and L. Xue, On the Ikehata theorem for H-separable skew polynomial rings, *Math. J. Okayama Univ.,* **40** 1998, 27–32.
[34] S. Yuan, Inseparable Galois theory of exponent one, *Trans. Amer. Math. Soc.,* **149** 1970, 163–170.

E-mail address: ikehata@ems.okayama-u.ac.jp